

[NT] Vulnerability in Print Spooler Service Allows Remote Code Execution (MS05-043)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0037.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/05

To: list@securiteam.com

Date: 10 Aug 2005 15:01:41 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Vulnerability in Print Spooler Service Allows Remote Code Execution
(MS05-043)

SUMMARY

A remote code execution vulnerability exists in the Printer Spooler service that allows an attacker who successfully exploited this vulnerability to take complete control of the affected system.

DETAILS

Affected Software:

Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=3DD3B530-7F43-4C18-8298-6E8797431A5D>>

Download the update

Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack

2 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=EF402946-1C3B-47E9-9D51-77D890DF8725>>

Download the update

Microsoft Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=25469675-DF28-4889-8D13-25EFCD498388>>

Download the update

Microsoft Windows Server 2003 for Itanium-based Systems –

Securiteam: [NT] Vulnerability in Print Spooler Service Allows Remote Code Execution (MS05-043)

<<http://www.microsoft.com/downloads/details.aspx?familyid=F0AEC064-34A3-4EE4-9F15-BE1E3DD02BC7>>
Download the update

Non-Affected Software:

- * Microsoft Windows XP Professional x64 Edition
- * Microsoft Windows Server 2003 Service Pack 1
- * Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- * Microsoft Windows Server 2003 x64 Edition
- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

CVE Information:

Print Spooler Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1984>>
CAN-2005-1984

Mitigating Factors for Print Spooler Vulnerability – CAN-2005-1984:

- * On Windows XP Service Pack 2 and Windows Server 2003, this vulnerability is restricted to authenticated users. Additionally, in order for this issue to create a remote attack vector on these operating system versions, a local user who has appropriate permissions must first share a printer or try to connect to a shared printer. If no user with appropriate permissions has shared a printer or tries to connect to a shared printer, an attacker would have to have valid logon credentials and must be able to log on locally to exploit this vulnerability.
 - * On Windows XP Service Pack 2 and Windows Server 2003, this issue would result in a denial of service condition. On Windows XP Service Pack 2 and Windows Server 2003, this issue cannot be exploited for remote code execution or for elevation of privilege.
- On other operating system versions, attacks attempting to exploit this vulnerability would most likely result in a denial of service condition. However remote code execution could be possible.
- * Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

Workarounds for Print Spooler Vulnerability – CAN-2005-1984:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

- * Disable the Print Spooler service

Disabling the Print Spooler service will help protect the affected system from attempts to exploit this vulnerability. To disable the Print Spooler service, follow these steps:

1. Click Start, and then click Control Panel. Alternatively, point to Settings, and then click Control Panel.
2. Double-click Administrative Tools.
3. Double-click Services.

Securiteam: [NT] Vulnerability in Print Spooler Service Allows Remote Code Execution (MS05-043)

4. Double-click Print Spooler.
5. In the Startup type list, click Disabled.
6. Click Stop, and then click OK.

You can also stop and disable the Print Spooler service by using the following command at the command prompt:

```
sc stop Spooler & sc config Spooler start= disabled
```

Impact of Workaround: If you disable the Print Spooler service, you cannot print locally or remotely. Therefore, we recommend this workaround only on systems that do not require printing.

* On Windows 2000 Server Service Pack 4 remove the Print Spooler service from the NullSessionPipes registry key:

Affected operating systems that are earlier than Windows 2000 Server Service Pack 4 allow anonymous connections to the affected service. To help prevent attempts to exploit this vulnerability by anonymous attackers, remove the Print Spooler Service from the NullSessionPipes subkey. This workaround will not prevent attacks from authenticated users. Use this workaround only if you cannot disable the Printer Spooler service.

Note Using Registry Editor incorrectly can cause serious problems that may require that you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. For information about how to modify the registry, view the "Change Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend backing up the registry before you modify it.

1. Click Start, click Run, type "regedt32" (without the quotation marks), and then click OK.
2. In Registry Editor, locate the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes
3. Edit the registry key and remove the SPOOLSS value.
4. Restart the affected system after performing these actions.

Impact of Workaround: Anonymous connections to the Print Spooler service will not be allowed. This is the default configuration of later operating system versions.

FAQ for Print Spooler Vulnerability – CAN-2005-1984:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could remotely take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. However, attempts to exploit this vulnerability could most likely result in a denial of service condition.

What causes the vulnerability?

An unchecked buffer in the Print Spooler service.

Securiteam: [NT] Vulnerability in Print Spooler Service Allows Remote Code Execution (MS05-043)

What is Print Spooler service?

The Print Spooler service, Spoolsv.exe, is an executable file that is installed as a service. The spooler is loaded when the operating system starts, and it continues to run until the operating system is shut down.

The Print Spooler service manages the printing process, which includes such tasks as retrieving the location of the correct printer driver, loading that driver, spooling high-level function calls into a print job, and scheduling print jobs. When the tasks for a particular print job are complete, the Print Spooler service passes the job to the print router.

For more information about the Print Spooler service, visit the following

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/d58ce7b9-49cf-4f5e-95e9-1a0> Web site.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability for remote code execution could take complete control of the affected system. On Windows XP Service Pack 2 and Windows Server 2003 this issue would result in a denial of service condition. On other operating system versions, attempts to exploit this vulnerability would most likely result in a denial of service condition. However remote code execution could be possible.

Who could exploit the vulnerability?

On Windows 2000 and Windows XP Service Pack 1, any anonymous user who could deliver a specially crafted message to the affected system could try to exploit this vulnerability. On Windows XP Service Pack 2 and Windows Server 2003, this vulnerability is restricted to authenticated users. An authenticated attacker may also be able to log on locally to a system and attempt to exploit this vulnerability on all affected operating system versions.

How could an attacker exploit the vulnerability?

An attacker could try to remotely exploit the vulnerability by creating a specially crafted message and sending the message to an affected system.

The message could then cause the affected system to execute code on operating system versions and configurations that were vulnerable to remote attack vectors. By default, Windows 2000 and Windows XP Service Pack 1 are vulnerable remotely. A remote attack vector cannot be created on Windows XP SP2 or on Windows Server 2003 unless a user who has appropriate permission shares a printer or tries to connect to a shared printer.

To locally exploit this vulnerability on all operating system versions, an attacker would first have to log on to the system. An attacker could then run a specially-crafted application that could exploit the vulnerability.

What systems are primarily at risk from the vulnerability?

Windows 2000 and Windows XP Service Pack 1 are primarily at risk from this vulnerability. Windows XP Service Pack 2 and Windows Server 2003 systems are at a reduced risk because of the additional mitigating factors that exist on these operating system versions. However, systems configured as Printer Servers are especially at risk to this vulnerability.

Securiteam: [NT] Vulnerability in Print Spooler Service Allows Remote Code Execution (MS05-043)

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your PC. End users can visit the <<http://go.microsoft.com/fwlink/?LinkId=21169>> Protect Your PC Web site. IT professionals can visit the <<http://go.microsoft.com/fwlink/?LinkId=21171>> Security Guidance Center Web site.

What does the update do?

The update removes the vulnerability by modifying the way that Print Spooler service validates the length of a message before it passes the message to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-043.msp>>
<http://www.microsoft.com/technet/security/Bulletin/MS05-043.msp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.